 Doc #1

UNITED STATES DISTRICT COURT

for the

District of New Hampshire

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)
THE PREMISES KNOWN AS 4 JANET LANE, NEWTON, NH, INCLUDING OUTBUILDINGS AND GARAGES LOCATED THEREON, A 2020 DODGE 1500 NH REG 364 2470, AND THE PERSON OF ANTHONY RIMAS

Case No. 1:21-MJ-51-01-AJ

APPLICATION FOR A WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location)*:

Please see attachment A.

located in the _____ District of New Hampshire, there is now concealed *(identify the person or describe the property to be seized)*:

Please see attachment B,

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☑ contraband, fruits of crime, or other items illegally possessed;
- ☑ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 U.S.C. § 2252(a)(2)	- Receipt and Attempted Receipt of Child Pornography
18 U.S.C.§ 2422(b)	- Attempted Enticement

The application is based on these facts:

Please see attached affidavit.

- ☑ Continued on the attached sheet.
- ☐ Delayed notice of _____ days *(give exact ending date if more than 30 days:* _____ *)* is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

/s/ Adam Rayho
Applicant's signature

TFO Adam Rayho, Homeland Security Investigations
Printed name and title

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by **Telephonic conference** *(specify reliable electronic means).*

Date: 03/10/2021

Andrea K. Johnstone
Judge's signature

City and state: Concord, New Hampshire

Hon. Andrea K. Johnstone, U.S. Magistrate Judge
Printed name and title

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF NEW HAMPSHIRE

IN THE MATTER OF THE SEARCH OF THE PREMISES KNOWN AS 4 JANET LANE, NEWTON, NH, INCLUDING OUTBUILDINGS AND GARAGES LOCATED THEREON, A 2020 DODGE 1500 NH REG 364 2470, AND THE PERSON OF ANTHONY RIMAS	Case No. 1:21-mj- 51-01-AJ **Filed Under Seal – Level II**

AFFIDAVIT IN SUPPORT OF APPLICATION FOR SEARCH WARRANT

I, Adam Rayho, a Task Force Officer with Homeland Security Investigations ("HSI"), being duly sworn, depose and state as follows:

1. I am a Detective with the Nashua Police Department (NPD) and have been a full time certified Police Officer in the State of New Hampshire since May 2014. I am currently assigned to the Special Investigations Division as a member of the Internet Crimes against Children (ICAC) Task Force and Homeland Security Investigations (HSI) as a Task Force Officer (TFO). My primary responsibility in this position is to investigate criminal offenses to include misdemeanor and felony level offenses, specifically cases of child exploitation. Prior to this assignment I was assigned to the Problem Oriented Policing (POP) Unit within the Narcotics Intelligence Division and the Patrol Division within the Uniform Field Operations Bureau.

2. As part of my duties, I have observed and reviewed examples of child pornography (as defined in 18 U.S.C. § 2256) in various forms of media, to include digital/computer media. During the course of this investigation, I have also conferred with other investigators who specialize in computer forensics and who have conducted numerous investigations which involved child sexual exploitation offenses.

3. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a warrant to search the premises located at 4 Janet Lane, Newton, NH (hereafter "SUBJECT PREMISES"), further described in Attachment A, including one residential dwelling; any computer, computer media, and electronic media located therein; a red 2020 Dodge 1500 NH Registration 364 2470 registered to Anthony Rimas (hereafter "SUBJECT VEHICLE") and the person of Anthony Rimas, for the things described in Attachment B– specifically, evidence, fruits, and instrumentalities of violations of Title 18, United States Code, Section 2252(a)(2), which relates to the illegal receipt of child pornography and attempt, and Title 18 United States Code. Section 2422(b), which relates to attempted online enticement of children.

4. During the course of this investigation I have conferred with other investigators who have conducted numerous investigations and executed numerous search and arrest warrants which involved child exploitation and/or child pornography offenses. This affidavit is intended to show only that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter. The facts set forth in this affidavit are based in part on my personal knowledge, information obtained during my participation in this investigation, information from others, including law enforcement officers, my review of documents and computer records related to this investigation, and information gained through my training and experience.

STATUTORY AUTHORITY

5. This investigation concerns alleged violations of 18 U.S.C. § 2252(a)(2), related to the receipt and attempted receipt of child pornography in the District of New Hampshire. 18 U.S.C. § 2252A(a)(2) makes it a crime for any person to knowingly receive or distribute any child

pornography (images of children under 18 engaging in sexually explicit conduct) that has been mailed, or using any means or facility of interstate or foreign commerce shipped or transported in or affecting interstate or foreign commerce by any means, including by computer. The statute also criminalizes attempt.

6. The investigation also concerns alleged violations of 18 U.S.C. § 2422(b), related to attempted online enticement. The statute makes it a crime to "knowingly persuade, induce, entice, or coerce any individual who has not attained the age of 18 years, to engage in prostitution or any sexual activity for which any person can be charged with a criminal offense" or to attempt to do so. In New Hampshire, it would be a crime for an adult male to engage in sexual acts with a 14-year-old child.

DEFINITIONS

7. "Child pornography" includes any visual depiction, including any photograph, film, video, picture, or computer or computer-generated image or picture, whether made or produced by electronic, mechanical, or other means, of sexually explicit conduct where (A) the production of the visual depiction involved the use of a minor engaged in sexually explicit conduct; (B) the visual depiction was a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaged in sexually explicit conduct; or (C) the visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaged in sexually explicit conduct. 18 U.S.C. § 2256(8).

8. "Child Erotica," as used herein, means materials or items that are sexually arousing to persons having a sexual interest in minors but that are not, in and of themselves, legally obscene or that do not necessarily depict minors in sexually explicit conduct.

9. "Computer," as used herein, is defined pursuant to 18 U.S.C. § 1030(e)(1) as "an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device. "These devices include but are not limited to any data-processing hardware (such as central processing units, memory typewriters, mobile "smart" telephones, tablets, and self-contained "laptop" or "notebook" computers).

10. "Computer hardware," as used herein, consists of all equipment which can receive, capture, collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, or similar computer impulses or data. Computer hardware includes any data-processing devices (including, but not limited to, central processing units, internal and peripheral storage devices such as fixed disks, external hard drives, floppy disk drives and diskettes, and other memory storage devices); peripheral input/output devices (including, but not limited to, keyboards, printers, video display monitors, and related communications devices such as cables and connections), as well as any devices, mechanisms, or parts that can be used to restrict access to computer hardware (including, but not limited to, physical keys and locks).

11. "Computer software," as used herein, is digital information which can be interpreted by a computer and any of its related components to direct the way they work. Computer software is stored in electronic, magnetic, or other digital form. It commonly includes programs to run operating systems, applications, and utilities.

12. "Computer-related documentation," as used herein, consists of written, recorded, printed, or electronically stored material which explains or illustrates how to configure or use computer hardware, computer software, or other related items.

13. "Computer passwords, pass-phrases and data security devices," as used herein, consist of information or items designed to restrict access to or hide computer software, documentation, or data. Data security devices may consist of hardware, software, or other programming code. A password or pass-phrase (a string of alpha-numeric characters) usually operates as a sort of digital key to "unlock" particular data security devices. Data security hardware may include encryption devices, chips, and circuit boards. Data security software of digital code may include programming code that creates "test" keys or "hot" keys, which perform certain pre-set security functions when touched. Data security software or code may also encrypt, compress, hide, or "booby-trap" protected data to make it inaccessible or unusable, as well as reverse the progress to restore it.

14. "Minor" means any person under the age of eighteen years. See 18 U.S.C. § 2256(1).

15. The terms "records," "documents," and "materials," as used herein, include all information recorded in any form, visual or aural, and by any means, whether in handmade form (including, but not limited to, writings, drawings, painting), photographic form(including, but not limited to, microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, photocopies), mechanical form (including, but not limited to, phonograph records, printing, typing) or electrical, electronic or magnetic form (including, but not limited to, tape recordings, cassettes, compact discs, electronic or magnetic storage devices such as floppy diskettes, hard disks, CD-ROMs, digital video disks ("DVDs"), Personal Digital Assistants ("PDAs"), Multi Media Cards ("MMCs"), memory sticks, optical disks, printer buffers, smart cards, memory calculators, electronic dialers, or electronic notebooks, as well as digital data files and printouts or readouts from any magnetic, electrical or electronic storage device).

16. "Sexually explicit conduct" means actual or simulated (a) sexual intercourse, including genital-genital, oral-genital, or oral-anal, whether between persons of the same or opposite sex; (b) bestiality; (c) masturbation; (d) sadistic or masochistic abuse; or (e) lascivious exhibition of the genitals or pubic area of any person. See 18 U.S.C. § 2256(2).

17. "Visual depictions" include undeveloped film and videotape, and data stored on computer disk or by electronic means, which is capable of conversion into a visual image. See 18 U.S.C. § 2256(5).

PROBABLE CAUSE

18. As a Detective in the Special Investigations Division working with the Internet Crimes against Children (ICAC) Task Force I maintain several online undercover ("UC") profiles, used in proactive investigations regarding the exploitation of children on the internet. The online undercover persona used during this investigation, was that of a 14-year-old female.

19. On October 15, 2020 I posted a message on Whisper[1] stating the following, "I hate high school :(". The message also displayed the following: Image of several school supplies in the background, Nickname: JH12, Sex: Other, Age: 18-20.

20. At approximately 2:05 p.m., I (hereafter referred to as "UC") received a message on Whisper from the user "whatthefckk" with the following profile information: Age: 36-44 years old, Sex: Male, Location: Seabrook, New Hampshire. During the first three messages on October 15, 2020, the UC advised "whatthefckk" she was 14 years old and "whatthefckk" acknowledged her age. Between October 15, 2020, and October 19, 2020, the UC communicated with "whatthefckk" on Whisper during which time "whatthefckk" advised he/she was 46 years old

[1] Whisper is a proprietary Android and iOS mobile app available for free download. It is a form of anonymous social media, allowing users to post and share photo and video messages anonymously.

and asked the UC if she had "ever played with an older man," which "whatthefckk" explained as "kiss, touch, etc." "whatthefckk" also asked the UC if she was "still a virgin" and asked her, "do you play with yourself?" Furthermore, "whatthefckk" advised the UC that she needed someone to teach her and asked if the UC wanted to learn, which "whatthefckk" specified to mean, "how to have an orgasm." Lastly, "whatthefckk" asked the UC if she ever had anyone come over her house when she was home alone.

21. On October 19, 2020 the UC provided "whatthefckk" her WhatsApp phone number and the conversation transitioned to the mobile messaging application WhatsApp. WhatsApp is a messaging platform owned by Facebook which requires users to sign up using their telephone number.

22. Beginning on October 19, 2020 and continuing until the week of March 8, 2021, the UC communicated with "whatthefckk" on WhatsApp. "whatthefckk" used the WhatsApp telephone number 978-330-6022 and the name "Jim." During this time period, the UC directly and indirectly reminded "Jim" of her age (14) several times by making statements such as, "Last yr in 8th grade," "Next yr when I turn 15," and "Just turned 14 a month ago," and "No lol I'm only 14."

23. Throughout the conversation, "Jim" discussed engaging in sexual acts with the UC on more than one occasion. Representative examples follow:

October 30, 2020
Jim: When we meet are you going to stroke and suck mine
Jim: I bet you will you are just nervous
UC: Do u want me to?
Jim: Of course i do

November 02, 2020
Jim: You want to have sex dont you
UC: Idk I've never done it
Jim: You want to try
UC: Ummm idc like with who

Jim: With me of course
UC: If u want to
UC: U don't care I'm younger n it would be my first time?
Jim: No i like the idea
Jim: You dont care that im older than your parents
Jim: What else do you want to try
UC: Like what else is there
UC: To do lol
Jim: You can suck my cock
Jim: I can lick your pussy
Jim: Try fingering your ass
UC: Ok lol u want to do all of those?
Jim: To start lol
UC: Ok lol

November 03, 2020
UC: Can I see what u look like
UC: I sent u a pic of me but u never sent me one
Jim: Its more risky for me
UC: Oh
UC: Why
Jim: How old are you hhhmmm
UC: 14
Jim: And im 46 lol
UC: No one looks at my phone
Jim: Think that could get me in trouble

November 05, 2020
Jim: So i can come over one day and we can play at your house
UC: Ya lol if u want to
Jim: We can have sex in your bed

November 16, 2020
Jim: Bet you wish you were playing with a cock
UC: Lmao
Jim: No?
UC: lol I've never done it
Jim: But you want to try dont you
UC: Like with who?
Jim: Like with me of course
UC: Oh
UC: Umm ya I'd try it with u if u want
Jim: Ill teach you what to do
UC: Ok how lol
Jim: How to stroke how to suck
Jim: How to take it in your pussy

24. On November 03, 2020, using the research database ZetX I searched the carrier information for the telephone number 978-330-6022, used by Jim on WhatsApp. Results of this search showed the carrier was Bandwidth.com which is a communications platform and service company. I subsequently emailed Bandwidth and asked what information the company would retain regarding the account associated with the phone number 978-330-6022. I later received an email from Bandwidth advising the telephone number I inquired about is on the Bandwidth network and assigned to the wholesale customer Pinger, Inc. I later researched Pinger, Inc., and learned the company is a US Telecom provider for free texts, pictures, calls, and voicemails. I later completed a search warrant for the Pinger, Inc. phone number 978-330-6022 which was signed by Hillsborough County Superior Court South Justice Jaclyn Colburn. The results of this search warrant contained the IP log for the number 978-330-6022 which contained IP addresses as recent as December 03, 2020. On December 03, 2020, between 01:53:23 UTC to 23:37:32 UTC the individual used three IP addresses. I received subpoena results for two of them: 174.255.65.199 and 75.68.0.18. The American Registry of Internet Numbers ("ARIN") identified these IP Addresses as belonging to Verizon Wireless ("Verizon") (174.255.65.199) and Comcast Cable Communications ("Comcast") (75.68.0.18). Further research showed the Pinger number used the Comcast IP 2,359 times from September 17, 2020 at 02:00:10 UTC until December 03, 2020 at 23:37:32 UTC. Based on my training and experience, this would indicate the IP is situated at the individual's home or work due to the amount of times it has been used.

25. HSI issued a summons to Verizon and Comcast to obtain subscriber information for the aforementioned IP Addresses. Result of the Comcast summons showed the subscriber was Anthony Rimas of 4 Janet Lane, Newton, New Hampshire, the SUBJECT PREMISES. Results of the Verizon summons showed the IP Address is a Natting IP, meaning multiple users can

connect to the same IP Address and are uniquely identified by their telephone number. In total, 420 users connected to the IP Address between December 03, 2020 and December 04, 2020.

26. Using the research database TLO, I observed the phone number associated with Rimas is (978) 430-0748. Furthermore, the Newton Police Department listed the phone number (978) 430-0748 as being used by Anthony Rimas on three occasions between 2013 and 2020. While reviewing the Verizon results from the natting IP address, I observed this phone number, (978) 430-0748, connected to the IP Address 174.255.65.199 four times as listed below:

12/3/2020 at 20:02 to 12/5/2020 at 03:54
12/3/2020 at 23:37 to 12/4/2020 at 00:22
12/3/2020 at 23:37 to 12/3/2020 at 23:54
12/3/2020 at 23:37 to 12/3/2020 at 23:56

27. As I was able to link Rimas to both IP addresses used by the WhatsApp number, I believe that he is the person identifying himself as "Jim" and speaking to the UC. On November 13, 2020 "Jim" suggested speaking with the UC on Zoom Video Communications Inc., aka "Zoom" and provided a meeting ID of 402 061 5216. Using an undercover, department issued laptop, I joined the zoom meeting but did not allow my video or audio to display/work. I proceeded to text "Jim" on WhatsApp as I heard him talking via Zoom. During this time I heard what appeared to be a male voice speaking to me. The conversation was not audio of video recorded.

28. On November 18, 2020 I completed a search warrant for the Zoom Video Communications meeting ID 402 061 5216 used on November 13, 2020, which was signed into effect by Hillsborough County Superior Court South Justice Charles Temple. I later received the results of the search warrant which produced investigative leads, to include the IP address 73.61.22.148, and email address, nunyaabizzz05@gmail.com, "Jim" used to create and start the Zoom meeting.

29. With the assistance of HSI I completed a summons to obtain subscriber information for the IP Address 73.61.22.148 which was identified using ARIN as belonging to Comcast. The initial response I received from Comcast indicated they were unable to provide subscriber information without a port number for the IP Address as the IP Address was assigned to the Xfinity Wi-Fi service. The original Zoom search warrant results identified the port number as 40803 thus a new summons was issued to Comcast. I later received the results of the second summons which showed the subscriber was Anthony Rimas of 4 Janet Lane, Newton, New Hampshire, the SUBJECT PREMISES. I also contacted Comcast who further described the IP Address as a "hot spot," thus it requires a user to provide their Comcast/Xfinity credentials to login and use the hot spot. Comcast furthered, the subscriber information provided was the credentials the user entered to login and use the hot spot.

30. On December 01, 2020 I completed a search warrant for the Google account nunyaabizzz05@gmail.com which was signed into effect by Hillsborough County Superior Court South Justice Charles Temple. I later received the results of the search warrant. During the UC's conversations with "Jim," he sent pictures which he purported to be of himself which were actually of the actor Pierce Brosnon. The google search results returned with the warrant included the following: *Nov 15, 2020, 5:44:19 PM UTC: Searched for pierce brosnan selfie holding up hand; Nov 15, 2020, 5:44:50 PM UTC: Searched for pierce brosnan selfie; Nov 16, 2020, 12:03:37 AM UTC: Searched for pierce brosnan selfie.*

31. During the month of December 2020, HSI issued a summons to Verizon to obtain subscriber information for the telephone number (978) 430-0748, which the Newton Police had linked to Rimas. I later received the results of the summons which stated *Please forward to reseller: Comcast Cable Communications, Inc.* Due to this information a second summons was

issued to Comcast to obtain subscriber information for the telephone number (978) 430-0748. I later received the results of the summons which showed the subscriber was Anthony Rimas of 4 Janet Lane, Newton, New Hampshire, the Subject Premises.

32. On January 12, 2021 "Jim" again asked the UC to join a Zoom Meeting. Prior to entering the meeting, I contacted New Hampshire Assistant Attorney General Nicole Clay and requested a one-party authorization to record the meeting between "Jim", Detective Abrams, and I. Detective Abrams assisted in the investigation by speaking with "Jim" during the Zoom meeting (audio only) and again informed "Jim" she was 14 years old. "Jim" proceeded to talk about having sexual intercourse with the UC and attempted to instruct her to "play" with her vagina. After the meeting, the following conversation took place (approximate):

UC: I was like confused
UC: Like if I had video what did u want me to do
Jim: Just rub at the right speed
Jim: Id tell you up down right left
UC: Like u would see my vagina?
UC: On the screen?
Jim: Yes
Jim: How else would i direct you

33. On February 03, 2021 during a conversation between "Jim" and the UC, "Jim" solicited and encouraged the UC to take a picture of her vagina and send it to him on WhatsApp. Approximate portions of the conversation are included below:

Jim: Working. Take any pics for me yet?
UC: No I haven't even tried to take my moms phone recently
Jim: Why not 😟
UC: Idk lol
UC: U like didn't tell me what u wanted
Jim: I want to see you naked 😁 *but any pic of you clothed is good*
UC: So like ummm if I took a nude like what would u want me to take it if?

Jim: Your body showing your tits your ass your pussy basically head to toe pic
UC: Lmao my vagina?
Jim: Yes 😁

Break in conversation

UC: How would I take the one of my vagina
Jim: You would need a mirror
Jim: Spread your legs and take a pic
UC: Oh ok
Jim: Too bad you cant vid chat
UC: Why?
Jim: We could see each other and you could watch me stroke my cock

34. On February 24, 2021 Rimas had the following conversation with the UC via WhatsApp:

Jim: Did you take a naked selfie?
UC: No do u want me to?
Jim: Of course i do 😁
UC: Like which ones
Jim: You naked standing is fine
UC: Umm ok I'll try
Jim: 😁
UC: Lol
Jim: You know i want that
UC: A nude?
Jim: Yes 😁
UC: Ya but like I wasn't sure like if u wanted that one or the other one u talked about
Jim: I want both
Jim: But regular nude will be easier
Jim: When can you zoom
UC: Like the one of my vagina?
Jim: Yes

35. On February 01, 2021 while searching for child exploitation groups on KIK messenger I observed a group titled NH D.aughters with the unique username #nhdau.ghterfantasy. Through my training and experience I recognized this group name could be associated with the exploitation of children.

36. Using an undercover KIK account and the persona of an adult male I joined the group. Between February 01, 2021 and continuing through the beginning of March 2021, I have observed several conversations within the group and have had private conversations with

members of the group which showed the majority of the members join or use the group to discuss the exploitation of children. One specific example is the user "jon240c." jon240c joined the group on February 16, 2021 and was a member until February 20, 2021. The user jon240c was identified by Detective J.B. Reid of the Boone North Carolina Police Department and North Carolina ICAC / Homeland Security Investigations as an individual producing child sexual abuse material involving his three year old daughter. On February 20, 2021, I along with members of Homeland Security Investigations and The Internet Crimes Against Children (ICAC) Task Force executed a search warrant on jon240c residence in Ossipee, New Hampshire and placed him under arrest.

37. On February 13, 2021, using an additional undercover KIK account and the persona of a 14-year-old female, I briefly joined the KIK group NH D.aughters with the unique username #nhdau.ghterfantasy. Almost immediately after joining I received a message from the KIK user "JJ" with the unique username "whatthefckk." I note that this is similar to the username of the Whisper profile previously discussed. This user is listed as the owner of the KIK NH D.aughters / #nhdau.ghterfantasy. Through my training and experience I know that the owner of a KIK group is either the individual who made the group or the longest active member after the original owner left the group. The owner of the group can make members of the group administrators which gives them the same privileges as the owner, such as adding individuals and removing them. The current rank structure of the KIK group #nhdau.ghterfantasy lists the owner as "JJ" unique username "whatthefckk" and administrator as "Jack Daniels" unique username "jackdan8578."

38. Starting on February 24, 2021, I communicated with KIK user whatthefckk via the private message feature. During my initial conversation I informed KIK user whatthefckk I was a

14-year-old female and he proceeded to ask questions and make statements such as "have you fucked an older man before…its time you did then." KIK user whatthefckk asked what had prompted me to join the group and I advised my friend had dared me. KIK user whatthefckk proceeded to ask if my friend and I would join a group chat with him. I gave KIK user whatthefckk the undercover KIK username of Detective Aaron Wojtkowski (Newbury MA Police Department), who uses the persona of a 13 year old female, and KIK user whatthefckk created a group chat involving the three of us titled "Jenni's chat."

39. From February 24, 2021 to March 04, 2021 Detective Wojtkowski and I communicated with KIK user whatthefckk in the group chat. During the group conversation KIK user whatthefckk asked questions like "who want to loose their virginity" and told the UCs, that he wanted to "get you naked and play" and that he wanted to have sex with them. He later told the UC that he would like to see pictures of her vagina.

40. Furthermore, on Friday March 05, 2021 KIK user whatthefckk provided Detective Wojtkowski with the number (978) 330-6022 to contact him. This is the same WhatsApp number I previously associated with Rimas.

41. The SUBJECT PREMISES is Rimas's registered address where I believe he resides with his wife and minor son. I saw him leaving from there on March 2, 2021 early in the morning.

COMPUTER ELECTRONIC STORAGE AND FORENSIC ANALYSIS

42. As described above and in Attachment B, this application seeks permission to search and seize records that might be found on the SUBJECT PREMISES and SUBJECT VEHICLE, in whatever form they are found. One form in which the records might be found is data stored on a computer's hard drive or other storage media. Thus, the warrant applied for would authorize the

seizure and search of electronic storage media or, potentially, the copying of electronically stored information, all under Rule 41(e)(2)(B).

43. I submit that if a computer or storage medium is found on the SUBJECT PREMISES, there is probable cause to believe those records will be stored on that computer or storage medium, for at least the following reasons:

a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

c. Wholly apart from user-generated files, computer storage media—in particular, computers' internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating systems or application operations, file system data structures, and

virtual memory "swap" or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

d. Similarly, files that have been viewed via the internet are sometimes automatically downloaded into a temporary internet directory or "cache."

e. Your Affiant is also aware, through training and experience, that digital storage devices have become interconnected, making it easy for even casual users of technology to transfer or copy images from one device to another, or to maintain duplicate copies on more than one device or storage medium. In fact, many devices such as smartphones can be set to automatically back up their contents to alternate storage facilities, such as laptop or desktop computers, another phone, photo-sharing websites, and cloud storage providers.

f. Your Affiant is aware that the contents of smart phones can be synched with or backed up to other digital devices in a variety of ways. Smartphones can be connected through cables to other devices, such as laptop computers, for data transfer. Smartphones can also connect to other devices and transfer photos or documents wirelessly through technology such as Bluetooth. Data can also be sent from the phone to an email account via the Internet, and subsequently downloaded from the Internet to a different device (such as a tablet, game system, or computer) for storage. In addition, many smartphones utilize "cloud" storage. Cellular telephones can be set to automatically back up their contents to user accounts hosted on servers of various cloud storage providers. Users can also opt to perform a back-up manually, on an as-needed basis. Your Affiant is aware that some smartphones also back up their contents automatically to

devices such as laptop computers. Additionally, cellular telephones can exchange data between two differing cellular communications devices and other types of electronic and media storage devices via Bluetooth or Wi-Fi, regardless of the type of operating system or platform being utilized to operate each of the electronic devices. In addition, media cards which contain many forms of data can be interchanged between multiple types of electronic devices, including but not limited to, different cellular telephones.

44. As set forth above, probable cause exists to believe that Rimas has attempted to receive child pornography by asking the UC who he thought was a 14-year-old girl to send him sexually explicit photographs of herself. Based upon my knowledge and experience in child pornography investigations, and the training and experience of other law enforcement officers with whom I have had discussions, I know that there are certain characteristics common to individuals involved in such crimes:

Those who distribute, transport, receive, or possess child pornography, or who attempt to commit these crimes may collect sexually explicit or suggestive materials, in a variety of media, including photographs, magazines, motion pictures, videotapes, books, slides and/or drawings or other visual media. Such individuals often times use these materials for their own sexual arousal and gratification.

b. Those who distribute, transport, receive, or possess child pornography, or who attempt to commit these crimes often possess and maintain copies of child pornography material, that is, their pictures, films, video tapes, magazines, negatives, photographs, correspondence, mailing lists, books, tape recordings, etc., in the privacy and security of their home or some other secure location. These individuals typically

retain pictures, films, photographs, negatives, magazines, correspondence, books, tape recordings, mailing lists, child erotica, and videotapes for many years.

c. Those who distribute, transport, receive, or possess child pornography, or who attempt to commit these crimes often maintain their collections that are in a digital or electronic format in a safe, secure and private environment, such as a computer and surrounding area. They often maintain these collections for several years and keep them close by, usually at the individual's residence, to enable the collector to view the collection, which is valued highly.

d. Those who distribute, transport, receive, or possess child pornography, or who attempt to commit these crimes also may correspond with and/or meet others to share information and materials; they rarely destroy correspondence from other child pornography distributors/collectors; they conceal such correspondence as they do their sexually explicit material; and they often maintain lists of names, addresses, and telephone numbers of individuals with whom they have been in contact and who share the same interests in child pornography.

45. As further described in Attachment B, this application seeks permission to locate not only computer files that might serve as direct evidence of the crimes described on the warrant, but also for forensic electronic evidence that establishes how computers were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence will be on any computer in the SUBJECT PREMISES accessible by RIMAS because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created.

b. Forensic evidence on a computer or storage medium can also indicate who has used or controlled the computer or storage medium. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, registry information, configuration files, user profiles, e-mail, e-mail address books, "chat," instant messaging logs, photographs, the presence or absence of malware, and correspondence (and the data associated with the foregoing, such as file creation and last-accessed dates) may be evidence of who used or controlled the computer or storage medium at a relevant time.

c. A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw conclusions about how computers were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, computer evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

46. Based on my training and experience I know that much of the media referenced above, which may contain contraband, fruits and evidence of crime, is by its very nature portable. This includes as example but is not limited to extremely compact storage devices such as thumb drives, laptop computers, and smart phones. In my training and experience, I know it is not uncommon for individuals to keep such media in multiple locations within their premises, including in outbuildings and motor vehicles, and/or on their person.

47. Searching storage media for the evidence described in the attachment may require a range of data analysis techniques. In most cases, a thorough search for information stored in storage media often requires agents to seize most or all electronic storage media and later review the media consistent with the warrant. In lieu of seizure, it is sometimes possible to make an image copy of storage media. Generally speaking, imaging is the taking of a complete electronic picture of the computer's data, including all hidden sectors and deleted files. Either seizure or imaging is often necessary to ensure the accuracy and completeness of data recorded on the storage media, and to prevent the loss of the data either from accidental or intentional destruction. This is true because of the following:

a. **The nature of evidence**. As noted above, not all evidence takes the form of documents and files that can be easily viewed on site. Analyzing evidence of how a computer has been used, what it has been used for, and who has used it requires considerable time, and taking that much time on premises could be unreasonable. As explained above, because the warrant calls for forensic electronic evidence, it is exceedingly likely that it will be necessary to thoroughly search storage media to obtain evidence, including evidence that is not neatly organized into files or documents. Just as a search of a premises for physical objects requires searching the entire premises for those objects that are described by a warrant, a search of this premises for the things described in this warrant will likely require a search among the data stored in storage media for the things (including electronic data) called for by this warrant. Additionally, it is possible that files have been deleted or edited, but that remnants of older versions are in unallocated space or slack space. This, too, makes it exceedingly likely that in this case it will be necessary to use more thorough techniques.

b. **The volume of evidence**. Storage media can store the equivalent of millions of pages of information. Additionally, a suspect may try to conceal criminal evidence; he or she might store it in random order with deceptive file names. This may require searching authorities to peruse all the stored data to determine which particular files is evidence or instrumentalities of a crime. This sorting process can take weeks or months, depending on the volume of data stored, and it would be impractical and invasive to attempt this kind of data search on-site.

c. **Technical requirements**. Computers can be configured in several different ways, featuring a variety of different operating systems, application software,

and configurations. Therefore, searching them sometimes requires tools or knowledge that might not be present on the search site. The vast array of computer hardware and software available makes it difficult to know before a search what tools or knowledge will be required to analyze the system and its data on-site. However, taking the storage media off-site and reviewing it in a controlled environment will allow its examination with the proper tools and knowledge.

d. **Variety of forms of electronic media.** Records sought under this warrant could be stored in a variety of storage media formats that may require off-site reviewing with specialized forensic tools.

48. Based on the foregoing, and consistent with Rule 41(e)(2)(B), when officers executing the warrant conclude that it would be impractical to review the hardware, media, or peripherals on-site, the warrant I am applying for would permit officers either to seize or to image-copy those items that reasonably appear to contain some or all of the evidence described in the warrant, and then later review the seized items or image copies consistent with the warrant. The later review may require techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of a hard drive to human inspection in order to determine whether it is evidence described by the warrant.

BIOMETRIC ACCESS TO DEVICES

49. This warrant seeks authorization for law enforcement to compel Anthony Rimas to unlock any DEVICES requiring biometric access subject to seizure pursuant to this warrant. Grounds for this request follow.

50. I know from my training and experience, as well as from information found in publicly available materials published by device manufacturers, that many electronic devices, particularly newer mobile devices and laptops, offer their users the ability to unlock the device through biometric features in lieu of a numeric or alphanumeric passcode or password. These biometric features include fingerprint scanners, facial recognition features and iris recognition features. Some devices offer a combination of these biometric features, and the user of such devices can select which features they would like to utilize.

51. If a device is equipped with a fingerprint scanner, a user may enable the ability to unlock the device through his or her fingerprints. For example, Apple offers a feature called "Touch ID," which allows a user to register up to five fingerprints that can unlock a device. Once a fingerprint is registered, a user can unlock the device by pressing the relevant finger to the device's Touch ID sensor, which is found in the round button (often referred to as the "home" button) located at the bottom center of the front of the device. The fingerprint sensors found on devices produced by other manufacturers have different names but operate similarly to Touch ID.

52. If a device is equipped with a facial-recognition feature, a user may enable the ability to unlock the device through his or her face. For example, this feature is available on certain Android devices and is called "Trusted Face." During the Trusted Face registration process, the user holds the device in front of his or her face. The device's front-facing camera then analyzes, and records data based on the user's facial characteristics. The device can then be unlocked if the front-facing camera detects a face with characteristics that match those of the registered face. Facial recognition features found on devices produced by other manufacturers have different names but operate similarly to Trusted Face.

53. If a device is equipped with an iris-recognition feature, a user may enable the ability to unlock the device with his or her irises. For example, on certain Microsoft devices, this feature is called "Windows Hello." During the Windows Hello registration, a user registers his or her irises by holding the device in front of his or her face. The device then directs an infrared light toward the user's face and activates an infrared-sensitive camera to record data based on patterns within the user's irises. The device can then be unlocked if the infrared-sensitive camera detects the registered irises. Iris-recognition features found on devices produced by other manufacturers have different names but operate similarly to Windows Hello.

54. In my training and experience, users of electronic devices often enable the aforementioned biometric features because they are considered to be a more convenient way to unlock a device than by entering a numeric or alphanumeric passcode or password. Moreover, in some instances, biometric features are considered to be a more secure way to protect a device's contents.

55. As discussed in this Affidavit, I have reason to believe that one or more digital devices will be found during the search. The passcode or password that would unlock the DEVICES subject to search under this warrant currently is not known to law enforcement. Thus, law enforcement personnel may not otherwise be able to access the data contained within the DEVICES, making the use of biometric features necessary to the execution of the search authorized by this warrant.

56. I also know from my training and experience, as well as from information found in publicly available materials including those published by device manufacturers, that biometric features will not unlock a device in some circumstances even if such features are enabled. This can occur when a device has been restarted, inactive, or has not been unlocked fora certain

period of time. For example, Apple devices cannot be unlocked using Touch ID when: (1) more than 48 hours has elapsed since the device was last unlocked; or, (2) when the device has not been unlocked using a fingerprint for 8 hours and the passcode or password has not been entered in the last 6 days. Similarly, certain Android devices cannot be unlocked with Trusted Face if the device has remained inactive for four hours. Biometric features from other brands carry similar restrictions. Thus, in the event law enforcement personnel encounter a locked device equipped with biometric features, the opportunity to unlock the device through a biometric feature may exist for only a short time.

57. In light of the foregoing, and with respect to (1) any device found on the person of Anthony Rimas, or (2) any device at/on SUBJECT PREMISES reasonably believed to be owned, used, or accessed by Anthony Rimas, law enforcement personnel seek authorization, during execution of this search warrant, to: (1) press or swipe the fingers (including thumbs) of Anthony Rimas to the fingerprint scanner of the seized device(s); (2) hold the seized device(s) in front of the face of Anthony Rimas and activate the facial recognition feature; and/or (3) hold the seized device(s) in front of the face of Anthony Rimas and activate the iris recognition feature, for the purpose of attempting to unlock the device(s) in order to search the contents as authorized by this warrant.

58. The proposed warrant does not authorize law enforcement to compel that an individual present at the SUBJECT PRESMISES state or otherwise provide the password or any other means that may be used to unlock or access the DEVICES. Moreover, the proposed warrant does not authorize law enforcement to compel an individual present at the SUBJECT PRESMISES to identify the specific biometric characteristics (including the unique finger(s) or other physical features) that may be used to unlock or access the DEVICES.

CONCLUSION

59. Based on the aforementioned factual information, I respectfully submit that there is probable cause to believe that evidence, fruits, and instrumentalities of the crime of receipt and attempted receipt of child pornography in violation of 18 U.S.C. § 2252(a)(2) and attempted enticement in violation of 18 U.S.C.§ 2422(b) may be located at the SUBJECT PREMISES. I therefore seek a warrant to search the SUBJECT PREMISES described in Attachment A and any computer and electronic media located therein, and to seize the items described in Attachment B.

60. I am aware that the recovery of data by a computer forensic analyst takes significant time; much the way recovery of narcotics must later be forensically evaluated in a lab, digital evidence will also undergo a similar process. For this reason, the "return" inventory will contain a list of only the tangible items recovered from the premises. Unless otherwise ordered by the Court, the return will not include evidence later examined by a forensic analyst.

Dated: March 10, 2021

Respectfully Submitted,

/s/ Adam Rayho
Adam Rayho
Task Force Officer
Homeland Security Investigations

The affiant appeared before me by telephonic conference on this date pursuant to Fed. R. Crim. P. 4.1 and affirmed under oath the content of this affidavit and application.

Andrea K. Johnstone

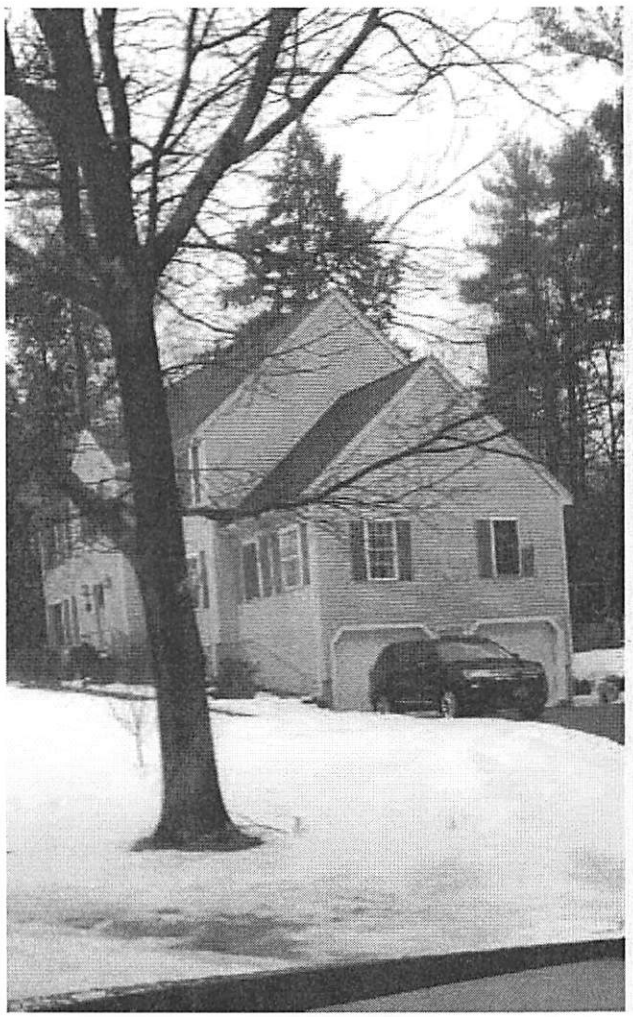
Hon. Andrea K. Johnstone
United States Magistrate Judge
Dated: March 10, 2021

ATTACHMENT A
PREMISES TO BE SEARCHED

The premises to be searched includes:

(1) The residential property located at 4 Janet Lane in Newton, NH is a single family residence with a white front door and a two car attached garage. The number 4 is clearly visible on the mailbox at the end of the driveway.
(2) A red 2020 Dodge 1500 NH Registration 364 2470 registered to Anthony Rimas
(3) The person of Anthony Rimas.

The following photographs depict the SUBJECT PREMISES:



ATTACHMENT B
ITEMS TO BE SEIZED

The following materials, which constitute evidence of the commission of a criminal offense, contraband, the fruits of crime, or property designed or intended for use or which is or has been used as the means of committing a criminal offense, namely violations of Title 18, United States Code, Sections 2252(a)(2) and 2422(b):

1. All records relating to violations of 18 U.S.C. §§2252(a)(2) and 2422(b) in any form wherever they may be stored or found at the SUBJECT PREMISES, including:
    a. records and visual depictions of minors engaged in sexually explicit conduct as defined in 18 U.S.C. § 2256;
    b. records or information pertaining to an interest in child pornography;
    c. communications with minor children or evidence of attempts to meet with minor children to engage in sexual activity;
    d. records or information pertaining to the receipt of visual depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256;
    e. records or information pertaining to use of the application Whisper, KIK, Pinger phone numbers, Gmail, and WhatsApp and the specific numbers and accounts referenced in the affidavit;
    f. records or information relating to the occupancy or ownership of the SUBJECT PREMISES, including, but not limited to, utility and telephone bills, mail envelopes, vehicle registrations, tax bills, and other correspondence.

2. Any computer or electronic media that were or may have been used by Anthony Rimas as a means to commit the offenses described on the warrant, including the receipt of child

pornography in violation of Title 18, United States Code, Section 2252(a)(2) or the attempted enticement of children in violation of Title 18, United States Code, Section 2422(b)

3. For any computer, computer hard drive, or other physical object upon which electronic data can be recorded (hereinafter, "COMPUTER") that is called for by this warrant, or that might contain things otherwise called for by this warrant:

a. evidence of who used, owned, or controlled the COMPUTER at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;

b. evidence of software that would allow others to control the COMPUTER, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

c. evidence of the lack of such malicious software;

d. evidence of the attachment to the COMPUTER of other storage devices or similar containers for electronic evidence;

e. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the COMPUTER;

f. evidence of the times the COMPUTER was used;

g. passwords, encryption keys, and other access devices that may be necessary to access the COMPUTER;

h. documentation and manuals that may be necessary to access the COMPUTER or to conduct a forensic examination of the COMPUTER;

i. contextual information necessary to understand the evidence described in this attachment;

j. evidence of the crimes described above in paragraph 1 including but not limited to images of child pornography, the use of messaging applications like Whisper, WhatsApp, KIK or other similar messaging/dating applications, communications with minors, evidence of attempts or plans to meet minors for sexual activity.

4. Records and things evidencing the use of the Internet, including:

a. routers, modems, and network equipment used to connect computers to the Internet;

b. records of Internet Protocol addresses used;

c. records of Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses.

5. DEVICE UNLOCK: During the execution of the search of the property described in Attachment A, and with respect to (1) any device on Anthony Rimas's person, or (2) any device at/on SUBJECT PREMISES reasonably believed to be owned, used, or accessed by Anthony Rimas, law enforcement personnel are authorized to (1) press or swipe the fingers (including thumbs) of Anthony Rimas to the fingerprint scanner of the seized device(s); (2) hold the seized device(s) in front of the face of Anthony Rimas and activate the facial recognition feature; and/or (3) hold the seized device(s) in front of the face of that Anthony Rimas and activate the iris recognition feature, for the purpose of

attempting to unlock the device(s) in order to search the contents as authorized by this warrant.

As used above, the terms "records" and "information" include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing, drawing, painting); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

As used above, the term "COMPUTER" includes but is not limited to any and all computer equipment, including any electronic devices that are capable of collecting, analyzing, creating, displaying, converting, storing, concealing, or transmitting electronic, magnetic, optical, or similar computer impulses or data. These devices include but are not limited to any data-processing hardware (such as central processing units, memory typewriters, mobile "smart" telephones, tablets, and self-contained "laptop" or "notebook" computers); internal and peripheral storage devices (such as fixed disks, external hard disks, floppy disk drives and diskettes, thumb drives, flash drives, Micro SD cards, SD cards, CDs, DVDs, tape drives and tapes, optical storage devices, zip drives and zip disk media, and other memory storage devices); peripheral input/output devices (such as keyboards, printers, fax machines, digital cameras, scanners, plotters, video display monitors, and optical readers); and related communications devices (such as modems, routers, cables and connections, recording equipment, RAM or ROM units, acoustic couplers, automatic dialers, speed dialers, programmable telephone dialing or

)signaling devices, and electronic tone-generating devices); as well as any devices, mechanisms, or parts that can be used to restrict access to such hardware (such as physical keys and locks).